

## 1 Description

2

3 Method for transmitting encrypted useful data objects

4

5 The present invention relates to a method for transmitting  
6 encrypted useful data objects (NDO) to a telecommunications  
7 terminal, such as a mobile telephone for example. The  
8 present invention relates more particularly to a method by  
9 means of which encrypted useful data objects can be  
10 transmitted to the telecommunications terminal in an  
11 efficient manner without the user of the telecommunications  
12 terminal incurring excessive or, as the case may be,  
13 excessively high charges.

14

15 A method or service for the reliable and accountable  
16 transmission of useful data objects to a telecommunications  
17 terminal, in particular a terminal implemented as a mobile  
18 radio device or mobile telephone, in a telecommunication  
19 network is under discussion at the present time. In this  
20 arrangement the transmission or even downloading of the  
21 useful data objects to the mobile radio device is to be  
22 performed using a protocol specified by the Open Mobile  
23 Alliance (OMA) or an internet protocol (e.g. Hypertext  
24 Transfer Protocol: http). A service for transmitting can in  
25 this case be specified such that it is to be made possible  
26 for a user with an application program which is available on  
27 the mobile radio device and which can be designated as a  
28 transmission client or, in the case of a pure downloading of  
29 data, as a download client, to transmit arbitrary useful  
30 data objects which are offered by one or more data  
31 provisioning components, in particular servers of service  
32 providers or content providers, in the data communications  
33 network.

1  
2 In this case the WAP forum or its successor organization  
3 Open Mobile Alliance (OMA) has defined various methods for  
4 managing explicit usage rights for digital content of any  
5 type, including for example multimedia data. It is provided  
6 here to apply restrictions to a useful data object that is  
7 to be transmitted with regard to its use by the recipient or  
8 user of the mobile radio device. This can be used, for  
9 example, to limit the number of uses of the useful data  
10 object or also to limit the period of use. The practical  
11 implementation is accomplished through the description of  
12 the restrictions by means of a corresponding language, such  
13 as, for example, ODRL (Open Digital Rights Language) or OMA  
14 DRM specified by the OMA, whereby the transmission client or  
15 another special application, a so-called DRM agent, receives  
16 the rights description for the purpose of managing the  
17 rights (DRM: Digital Rights Management) linked to a  
18 (digital) useful data object, evaluates same, stores it on  
19 the mobile radio device in a protected memory area that is  
20 not accessible to the user and, in the case of a request  
21 from the user to use the object, grants or does not grant  
22 rights in accordance with the rights description. The  
23 useful data object itself can be protected against  
24 unauthorized access either by being stored in encrypted form  
25 in a freely accessible memory area on the mobile radio  
26 device or by being managed by a special application, for  
27 example the DRM agent, which allows no unauthorized access  
28 to the object by the user.

29  
30 According to a variant specified by the Open Mobile  
31 Alliance, referred to as "separate delivery", for the  
32 management of DRM-protected contents, a useful data object  
33 provided by a data provisioning component is packed in

1 encrypted form and for the purpose of transport and for  
2 storage onto a telecommunications terminal, such as a mobile  
3 radio device, in a so-called container file or a so-called  
4 container object (which has been assigned for example the  
5 data type or content type  
6 "Application/VND.OMA.DRM.Content"). With a service for the  
7 reliable transmission of content from a data provisioning  
8 component (content download), the encrypted useful data  
9 object, packed in the container object using WAP protocols  
10 (such as for example the WSP: Wireless Session Protocol) or  
11 internet protocols (such as for example http), is  
12 transmitted to the telecommunications terminal. A so-called  
13 rights object is transmitted separately from the encrypted  
14 useful data object via a secure channel to the  
15 telecommunications terminal, for example automatically by  
16 means of WAP push. The rights object contains a description  
17 of the rights granted to the user for use of the encrypted  
18 useful data object, a reference to the container object  
19 enabling the rights object to be assigned to the  
20 corresponding container object, and a key with which the  
21 encrypted useful data object can be decrypted so that it can  
22 subsequently be used. A special device or application, which  
23 may be the aforementioned DRM agent, is required on the  
24 telecommunications terminal, such as the mobile radio  
25 device, in order to use the combination of the encrypted  
26 useful data object packed in the container object and the  
27 rights object. After the rights object has been transmitted  
28 to the telecommunications device the rights object is  
29 transferred directly to the DRM agent, which is responsible  
30 for managing and keeping the secret, i.e. the key for  
31 decrypting the encrypted useful data object. In practice the  
32 DRM agent stores the rights object on the telecommunications  
33 terminal and protects it against an unauthorized access by

1 other applications or users. When an encrypted useful data  
2 object is to be used, the DRM agent is activated first. The  
3 DRM agent searches for a rights object matching the  
4 container object in the memory area managed by it in the  
5 telecommunications device with the aid of the identification  
6 contained in the container object and also in the rights  
7 object, checks whether rights can be granted for the  
8 requested type of use (such as, for example, "playing back"  
9 music data or "displaying" image data, etc.) and, if the  
10 rights can be granted, decrypts the useful data object using  
11 the key from the rights object. With the above described  
12 method, in which an encrypted useful data object and a  
13 rights object separate therefrom can be used, the value of  
14 digital data is no longer represented by the (encrypted)  
15 useful data object or the container object itself, but  
16 rather by the rights object and the key contained therein,  
17 without which, of course, the encrypted useful data object  
18 cannot be used. Thus, in this case, the encrypted useful  
19 data objects can be stored packed in the container objects  
20 in a freely accessible manner on the telecommunications  
21 terminal.

22  
23 Since, as already mentioned, the (encrypted) useful data  
24 objects that are to be transmitted can be data objects with  
25 multimedia contents and consequently data having a large  
26 volume, a service providing large transmission capacity is  
27 required for a corresponding transmission of such data. The  
28 Multimedia Messaging Service (MMS) specified by the 3GPP  
29 (3rd Generation Partnership Project) and by the OMA, for  
30 example, has the capability to perform the switching and  
31 transmission of multimedia messages to and from mobile  
32 communications subscribers.

1 A combination of the two techniques DRM and MMS is therefore  
2 beneficial. With MMS, valuable digital content can be  
3 transmitted to other subscribers; at the same time the  
4 actual usage rights for the content can be defined and  
5 likewise transmitted. For this purpose the content is packed  
6 in the DRM container objects and optionally encrypted  
7 (depending on the chosen DRM method). The use of the content  
8 can thus be restricted to the addressed recipient(s) of the  
9 MMS message and, for example, an undesirable further  
10 distribution by simple forwarding of a message by the first  
11 recipient can be prevented. A further possibility is the  
12 forwarding of the encrypted content by a first MMS recipient  
13 to a second MMS recipient, a practice referred to as  
14 superdistribution. Independently of the transport of the  
15 encrypted content, both recipients must in this case receive  
16 rights separately from the rights provider in order to be  
17 able to decrypt and use the encrypted content.

18  
19 The forwarding (superdistribution) of encrypted contents NDO  
20 contained in a DRM-protected container object CO from a  
21 first MMS recipient (in this case the sender) TG1 with a  
22 sending MMS user application SNA to a second MMS recipient  
23 TG2 with a receiving MMS user application ENA via an MMS  
24 switching component VK consisting of a sender-side MMS  
25 switching unit SMV and a recipient-side MMS switching unit  
26 EMV, as shown in Fig. 1, is altogether desired by the  
27 providers, since via this mechanism the contents are  
28 distributed among the users and each user must individually  
29 download a rights object if he or she wishes to gain access  
30 to the DRM-protected content. The downloading of a rights  
31 object from a server of a rights provider by a subscriber  
32 after receiving the DRM-protected content by MMS can be

1 charged by the provider. In other words additional revenue  
2 can be generated.

3  
4 In this case, however, the problem arises that the protected  
5 content is encrypted and the MMS switching units have no  
6 access to the content. In particular the otherwise possible  
7 and frequently practiced adaptation of the content of a  
8 multimedia message to the characteristics or capabilities  
9 with regard to the processing of the receiving MMS user  
10 application ENA and of the terminal device on which said  
11 processing is performed is consequently not possible. There  
12 exists the increased risk that a DRM-protected content which  
13 leaves the recipient-side MMS switching unit EMV in a  
14 multimedia message in unmodified form and without being  
15 controlled en route to the receiving terminal device cannot  
16 be used on the latter. This is all the more critical if the  
17 user of the receiving terminal device downloads a rights  
18 object matching the content object for a charge onto his or  
19 her mobile terminal device and discovers only after the  
20 downloading and invoicing associated therewith that the  
21 contents are not suitable for the terminal device or cannot  
22 be used or can be used only with restrictions.

23  
24 It is therefore the object of the present invention to  
25 create a means of transmitting an encrypted useful data  
26 object to a telecommunications terminal, wherein the  
27 telecommunications terminal's ability to process or use said  
28 object is assured.

29  
30 This object is achieved by the independent claims.  
31 Advantageous embodiments are the subject matter of the  
32 dependent claims.

1 In this arrangement a method for transmitting encrypted  
2 useful data objects to a first telecommunications terminal  
3 comprises the following steps. Firstly, in a switching  
4 component of a telecommunications network an encrypted  
5 useful data object that is to be transmitted to the first  
6 telecommunications terminal is provided with a reference. In  
7 this case the encrypted useful data object may previously  
8 have been provided with a reference by a data provisioning  
9 component (of a content provider or useful data object  
10 provider), the reference serving to contact the data  
11 provisioning component (or possibly another defined data  
12 provisioning component). The reference can be used for  
13 obtaining the description of the characteristics of the  
14 encrypted useful data object or for requesting the data  
15 provisioning component to check the suitability of the  
16 useful data object for a telecommunications terminal. In  
17 particular the encrypted useful data object can here be  
18 contained in a container object, such as a DRM container, in  
19 which the reference is also provided. If a switching  
20 component of a telecommunications network receives an  
21 encrypted useful data object with a reference for  
22 transmission to a first telecommunications terminal, said  
23 switching component uses the reference to contact the  
24 specified data provisioning component and check the  
25 suitability of the useful data object for the (first)  
26 telecommunications terminal. The switching component first  
27 determines a profile relating to the capability of the first  
28 telecommunications terminal to process a useful data object.  
29 The switching component also transmits a request together  
30 with the determined profile of the first telecommunications  
31 terminal to a data provisioning component (in particular of  
32 the provider of the useful data objects) according to an  
33 address contained in the reference in order to check whether

1 the useful data object to be transmitted can be processed by  
2 the first telecommunications terminal. Next, information  
3 concerning the check by the switching component is  
4 communicated by the data provisioning component and an  
5 encrypted useful data object is provided by the switching  
6 component in accordance with the information concerning the  
7 check and the first telecommunications terminal is notified  
8 of this.

9  
10 According to an advantageous embodiment the described method  
11 for transmitting encrypted useful data objects is performed  
12 in accordance with the Multimedia Messaging Service (MMS).  
13 This enables the transmission of (encrypted) useful data  
14 objects which can also include multimedia content having a  
15 large data volume, such as digital photographs or video  
16 clips.

17  
18 According to an advantageous embodiment the method for  
19 transmitting encrypted useful data objects can then appear  
20 as follows.

21  
22 1. During the generation of an encrypted useful data object,  
23 a provider of contents or of useful data objects integrates  
24 into a container object for the DRM-protected useful data  
25 object an additional reference for use by a switching  
26 component of a telecommunications network, in particular an  
27 MMS switching unit, for the functionality described below.

28  
29 2. It is assumed that a user of a further telecommunications  
30 terminal would like to transmit an above described useful  
31 data object, either encrypted or provided in a container  
32 object, via the switching component to the aforementioned  
33 first telecommunications terminal. For this purpose the



1 encrypted useful data object to be transmitted is first sent  
2 to the switching component and is now available there for  
3 further processing. The switching component, which in  
4 particular within the framework of the MMS has a recipient-  
5 side MMS switching unit which is assigned to the first  
6 telecommunications terminal to which the encrypted useful  
7 data object is to be transmitted, checks the content of the  
8 useful data object for the delivery to a receiving user  
9 application on the receiving telecommunications terminal.  
10 The encrypted useful data object is in this case to be  
11 delivered by means of a delivery message, in particular by  
12 means of a multimedia message (MM) within the framework of  
13 the MMS, which has to be prepared.

14  
15 3. The switching component (recipient-side MMS switching  
16 unit) analyzes the delivery message (MM) with regard to  
17 encrypted useful data objects or DRM container objects (with  
18 useful data objects) contained therein and a respective  
19 existence of signaling information or a reference, as has  
20 been explained under point 1. The reference can in this case  
21 be an address, for example in the form of a Uniform Resource  
22 Locator (URL). This reference or address, if present, is  
23 extracted from the DRM container object (encrypted useful  
24 data object).

25  
26 4. The switching component (recipient-side MMS switching  
27 unit) determines the characteristics or capabilities of the  
28 first (receiving) telecommunications terminal on which the  
29 receiving MMS user application is executed. This can be  
30 effected either by means of a query to a database in the  
31 area of the switching component (recipient-side MMS  
32 switching unit) or a further component of the  
33 telecommunications network of the network operator, to which

1 the user of the first telecommunications terminal in  
2 particular is assigned as a customer. Alternatively the  
3 switching component (recipient-side MMS switching unit) can  
4 establish direct contact with the first telecommunications  
5 terminal on which the MMS user application is executed and,  
6 via this contact, query the characteristics or capabilities  
7 of the telecommunications terminal in respect of the  
8 processing of useful data objects.

9  
10 5. The switching component (recipient-side MMS switching  
11 unit) inquires of a data provisioning component of the  
12 content provider via the corresponding reference (URL) in  
13 the DRM container whether the encrypted content or the  
14 encrypted useful data object is suitable for the receiving  
15 terminal device, i.e. can also be used on the latter. In  
16 this case the switching component (recipient-side MMS  
17 switching unit) integrates the profile information relating  
18 to the processing capabilities of the receiving  
19 telecommunications terminal into the request. In the  
20 request, the DRM-protected content itself can also  
21 optionally be transmitted to the data provisioning component  
22 by the MMS switching unit, as a result of which a content  
23 provider is relieved of the need to hold every content or  
24 every useful data object in readiness on a permanent basis.

25  
26 6. The data provisioning component analyzes the request and,  
27 contained therein, the profile characteristics of the  
28 telecommunications terminal (referred to in the following as  
29 the target terminal device) on which the DRM-protected  
30 content is to be used.

31  
32 7. The data provisioning component then answers the  
33 switching component (recipient-side MMS switching unit) with

1 a message including information which either indicates that  
2 the content is suitable for the target terminal device or  
3 that it is not suitable. This message optionally contains a  
4 pointer for the downloading of the suitable content or  
5 useful data object from a data provisioning component or the  
6 suitable content or suitable useful data object in DRM-  
7 protected form itself. This is useful in particular if the  
8 original content was not suitable for the target terminal  
9 device.

10  
11 8. The switching component (recipient-side MMS switching  
12 unit) takes the information received into account as  
13 appropriate, composes or provides the delivery message (in  
14 particular MM) with suitable objects for downloading by the  
15 MMS user application and sends a recipient notification (in  
16 particular MMS recipient notification conforming to a  
17 conventional MMS method) to the first telecommunications  
18 terminal, where the notification is processed by a  
19 corresponding user application (MMS user application).

20  
21 9. The remainder of the procedure can be implemented in a  
22 conventional manner. Subsequently to the recipient  
23 notification, the user application (MMS user application) on  
24 the first telecommunications terminal requests the delivery  
25 message (MM) from the switching component (recipient-side  
26 MMS switching unit). For the DRM-protected objects in the  
27 delivery message (MM), the offering of a rights provider can  
28 be accepted for example via a corresponding browser of the  
29 first telecommunications terminal and one or more  
30 corresponding rights objects can be loaded - possibly  
31 independently of MMS - by a rights provisioning component  
32 (server) of the rights provider onto the first  
33 telecommunications terminal, as a result of which access to

1 and use of the DRM-protected contents in the suitable format  
2 is then finally made possible on the terminal device.

3  
4 To sum up, an essential aspect of the explained embodiment  
5 is therefore the additional signaling (by the provider of  
6 contents or useful data objects) in the container for the  
7 DRM-protected or encrypted content, by means of which  
8 signaling firstly a reference for the use of the above  
9 explained functionality is integrated into the container and  
10 secondly the support of the provider of contents or useful  
11 data objects using the data provisioning component for this  
12 additional functionality is signaled. Furthermore the  
13 switching component (recipient-side MMS switching unit) is  
14 assigned the additional functionality to examine DRM  
15 containers with regard to the above described signaling and  
16 initiate a corresponding communication with the provider of  
17 contents or useful data objects or the associated data  
18 provisioning component. The switching component (recipient-  
19 side MMS switching unit) also receives the additional  
20 functionality to determine the characteristics or processing  
21 capabilities of the recipient terminal device and integrate  
22 them into the request to the data provisioning component.  
23 The data provisioning component receives a further essential  
24 functionality, i.e. to check the suitability of the DRM-  
25 protected content for the receiving telecommunications  
26 terminal and where necessary provide a better matching  
27 content or a suitable useful data object.

28  
29 According to an advantageous embodiment the first  
30 telecommunications terminal and possibly further  
31 telecommunications terminals as well as the switching  
32 component are part of a telecommunications network. In this  
33 case the telecommunications terminal or the further

1 telecommunications terminals can be part of a first  
2 telecommunications network (in the case of a plurality of  
3 telecommunications terminals, however, these do not have to  
4 be part of the same telecommunications network). Accordingly  
5 the switching component, which is embodied in particular as  
6 a server of a data transmission service, such as, for  
7 example, as an MMS relay server, can be provided in a second  
8 telecommunications network which is connected to the  
9 telecommunications network(s) which is (are) assigned to the  
10 telecommunications terminal or the further  
11 telecommunications terminals. This second telecommunications  
12 network can be implemented in particular as a  
13 telecommunications network based on internet protocols, such  
14 as the Hypertext Transfer Protocol. It is furthermore  
15 conceivable that the data provisioning component is also  
16 provided in the second telecommunications network or in a  
17 further telecommunications network connected to said second  
18 network.

19  
20 In order to be able to use the method for transmitting  
21 useful data objects with maximum flexibility, the  
22 telecommunications terminal (or also the further  
23 telecommunications terminals) can preferably be embodied as  
24 a mobile telecommunications terminal. In particular it is  
25 conceivable that the data or messages to and from the first  
26 or the further telecommunications terminal are sent via an  
27 air interface. In this case the respective  
28 telecommunications terminal can include a radio module. The  
29 telecommunications terminal can be embodied, for example, as  
30 a mobile telephone, as a cordless telephone, as a smartphone  
31 (combination of a small portable computer and a mobile  
32 telephone), as a PDA (PDA: Personal Digital Assistant) or as  
33 an organizer. Furthermore the telecommunications terminal

1 can also comprise other devices that are accessible by  
2 mobile means, such as a personal computer (PC) or a laptop  
3 which can be reached via a mobile radio network by means of  
4 a connected mobile radio device (mobile telephone or mobile  
5 radio module). The mobile radio device can then be connected  
6 to the personal computer or laptop for example via a cable  
7 or can also make contact with these wirelessly via an  
8 infrared interface or a local Bluetooth network.

9  
10 As already mentioned, the transmission of data and messages  
11 to and from the respective telecommunications terminal can  
12 then be effected using WAP protocols or the Hypertext  
13 Transfer Protocol (http). In this case a telecommunications  
14 terminal, such as the mobile radio device, including the  
15 telecommunications network assigned thereto and embodied in  
16 the form of a mobile radio network can operate in accordance  
17 with the GSM (Global System for Mobile Communication)  
18 standard or the UMTS (Universal Mobile Telecommunications  
19 System) standard etc. Such mobile radio networks or  
20 telecommunications devices conforming to the GSM or UMTS  
21 standard can represent a platform for WAP protocols or for  
22 the WAP protocol stack (WAP: Wireless Application Protocol)  
23 by means of which data (messages or useful data objects) can  
24 be transmitted in the respective mobile radio network.

25  
26 Advantageously the first and the second telecommunications  
27 network are connected to one another by means of a  
28 connection component. In the case of the use of the WAP  
29 protocol stack, as mentioned above, it is possible, through  
30 the use of a WAP gateway as an interface or connection  
31 component between a mobile radio network and another  
32 network, for example a network based on an internet  
33 protocol, to create a connection to this network. In this

1 way it is possible for the switching component to be located  
2 in a network based on an internet protocol, such as the  
3 internet, in which case the data (messages, useful data  
4 objects) can be transmitted via a WAP gateway and finally  
5 via an air interface of a mobile radio network between the  
6 base station or base stations of the mobile radio network  
7 and to the respective telecommunications terminals of users.  
8 It should be mentioned in this context that, in particular  
9 within the framework of the MMS data transmission service,  
10 messages can be sent by an MMS relay server as part of a  
11 switching component automatically, i.e. without a request  
12 from a telecommunications terminal, to a telecommunications  
13 terminal by means of WAP push. In this case the MMS relay  
14 server serves as a so-called push initiator which causes the  
15 WAP gateway or a subcomponent thereof, namely the push proxy  
16 gateway, to send a message by WAP push to the  
17 telecommunications terminal. According to the MMS  
18 transmission service, for example, the recipient  
19 notification is transmitted to the first telecommunications  
20 terminal by means of WAP push.

21  
22 According to an advantageous embodiment, the useful data  
23 objects can be data in the form of text data, image data or  
24 video data, audio data, executable programs or software  
25 components, or a combination of these data types, i.e.  
26 multimedia data or content.

27  
28 According to a further aspect, a telecommunications  
29 arrangement comprising a switching component, a data  
30 provisioning component, and at least one first  
31 telecommunications terminal is created, with the  
32 telecommunications arrangement being embodied to perform an  
33 above-mentioned method.

1  
2 Preferred embodiments of the present invention are explained  
3 in more detail below with reference to the accompanying  
4 drawings, in which:

5  
6 Fig. 1 shows a block diagram of a conventional MMS  
7 architecture for the transmission of useful data objects  
8 from a telecommunications terminal via a switching component  
9 to a further telecommunications terminal;

10  
11 Fig. 2 shows a block diagram of a telecommunications  
12 arrangement in which the message flow during the  
13 transmission of an encrypted useful data object according to  
14 a preferred embodiment of the invention is represented;

15  
16 Fig. 3 shows a schematic representation of a container  
17 object according to an embodiment of the invention.

18  
19 Reference is made to Fig. 2, which illustrates a message  
20 flow between components of a telecommunications arrangement  
21 during the transmission of an encrypted useful data object  
22 to a telecommunications terminal according to a preferred  
23 embodiment of the invention.

24  
25 As can be seen in Fig. 2, the telecommunications arrangement  
26 for performing a method for transmitting useful data objects  
27 by means of the MMS comprises a switching component VK  
28 consisting of a sender-side MMS switching unit SMV, which is  
29 assigned to a sending telecommunications terminal (not  
30 shown, but refer to the telecommunications terminal TG1 of  
31 Fig. 1), and a recipient-side MMS switching unit EMV, which  
32 is assigned to a receiving telecommunications terminal TG2.  
33 In this arrangement the two telecommunications terminals are



1 embodied for example as mobile telephones which can operate  
2 according to the UMTS standard. It is further assumed that  
3 the telecommunications terminal TG2 embodied as a mobile  
4 telephone (as also the (not shown) sending  
5 telecommunications terminal) is part of a mobile radio  
6 network. The mobile telephone TG2 is able to use WAP  
7 protocols (e.g. Wireless Session Protocol: WSP, etc.) or the  
8 WAP protocol stack in order to transmit data via an air  
9 interface to a corresponding stationary send/receive  
10 arrangement of the mobile radio network assigned to the  
11 mobile telephone TG2. In addition, the telecommunications  
12 arrangement comprises a database DBE, in which profiles of  
13 telecommunications terminals relating to the processing  
14 capabilities or processing characteristics of useful data  
15 objects are stored, a data provisioning component DBK of a  
16 provider of contents or useful data objects, and a rights  
17 provisioning component RBK of a provider of rights objects  
18 associated with the respective useful data objects (the  
19 provider of rights objects and the provider of useful data  
20 objects may be identical here). At the same time the  
21 database DBE, the data provisioning component DBK and the  
22 rights provisioning component RBK can be provided in the  
23 mobile radio network assigned to the mobile telephone TG2 or  
24 can be provided for example in the internet, which is  
25 connected to the mobile radio network of the mobile  
26 telephone TG1 via corresponding WAP gateways.

27  
28 In the following description it is assumed according to Fig.  
29 1 that there is provided on the mobile telephone TG2 an MMS  
30 user application or MMS user application ENA via which the  
31 mobile telephone TG2 communicates with the MMS switching  
32 unit EMV and the rights provisioning component RBK.

1 The signaling or message flow during the  
2 transmission/delivery of a multimedia message MM with DRM-  
3 protected content or useful data object NDO to the MMS user  
4 application ENA on the target terminal device or mobile  
5 telephone TG2 shall now be explained in accordance with a  
6 preferred embodiment of the invention. The information or  
7 message flow is symbolized by the arrows in the block  
8 diagram and described with reference to the assigned  
9 numbers:

10  
11  
12 1. An encrypted useful data object, i.e. a useful data  
13 object NDO provided in a DRM container object CO, is  
14 transmitted by the sender-side MMS switching unit SMV to the  
15 recipient-side MMS switching unit EMV (cf.  $\alpha$ ). It is assumed  
16 here that the encrypted useful data object has previously  
17 been sent for example by a further telecommunications  
18 terminal assigned to the sender-side MMS switching unit SMV  
19 (refer, for example, to the telecommunications terminal TG1  
20 of Fig. 1) by means of a multimedia message for forwarding  
21 to the mobile telephone TG2. However, a plurality of  
22 (encrypted or DRM-protected) useful data objects may also be  
23 contained in a multimedia message of this type.

24  
25 2. The MMS switching unit EMV queries a database DBE for the  
26 characteristics or capabilities of the target terminal  
27 device TG2 with the receiving MMS user application ENA (cf.  
28  $\sigma$ ). A database of this kind can be attached to an MMS  
29 switching unit or be provided as a separate component in a  
30 telecommunications network which is connected to the MMS  
31 user application ENA. In it, the MMS switching unit can  
32 create one or more data records for the terminal devices  
33 used by the user individually for an individual MMS user. If

1 there exists for the MMS switching unit EMV a means of  
2 accessing the information known in the mobile radio network  
3 (of the telecommunications terminal or mobile telephone TG2)  
4 regarding with which telecommunications terminal a user in  
5 the mobile radio network has registered, the MMS switching  
6 unit EMV can query the corresponding profile information for  
7 the terminal device from the database DBE. A requirement for  
8 this is that a profile for the currently used terminal  
9 device has already been stored in the database, i.e. that  
10 the MMS switching unit EMV has already communicated once  
11 with the MMS user application ENA on the currently used  
12 target terminal device of the user.

13

14 3. As an alternative to the query under point 2., the MMS  
15 switching unit EMV queries the target terminal device TG2  
16 directly for the characteristics (cf. 8). For this purpose  
17 the MMS switching unit EMV triggers the MMS user application  
18 ENA on the target terminal device TG2 to transmit the  
19 characteristics or capabilities of the target terminal  
20 device TG2 in the form of profile information to the MMS  
21 switching unit EMV. The trigger can be implemented for  
22 example by means of a push message by WAP push or via a  
23 specially formatted/coded short message in the "Short  
24 Message Service" SMS. The response can be effected for  
25 example by "http-Post-Request", with the profile information  
26 being integrated as useful data, or an "http-GET-Request" is  
27 sent which contains the profile information of the terminal  
28 device in the form of "http-Accept-Header-Fields" or in the  
29 form of a "WAP-User Agent-Profile". The response to the  
30 requests can either be omitted or return a simple status  
31 value to the target terminal device TG2. The address to  
32 which such a message can be sent by the target terminal  
33 device TG2 to the MMS switching unit EMV is sent in the

1 first trigger message from the MMS switching unit to the  
2 target terminal device TG2. Since this functionality is of  
3 very fundamental importance also to other services and  
4 applications, the communication between target terminal  
5 device and a unit in the network can also be effected by  
6 another unit in the network instead of by the MMS switching  
7 unit. This can also be e.g. a proxy or a WAP push proxy  
8 gateway (PPG). After determining the characteristics of the  
9 target device, the MMS switching unit EMV can store the  
10 characteristics of the target terminal device TG2 as a  
11 profile in the database DBE according to point 2. in order  
12 to have the information available for future transactions  
13 with the target terminal device without again having to  
14 initiate a direct transfer of the information from the  
15 target terminal device TG2 to the network. In this way  
16 savings in terms of time, transmission capacity and costs  
17 can be made for the user.

18  
19 4. Based on the information obtained in points 2. and 3.  
20 with regard to the characteristics of the target terminal  
21 device TG2, the MMS switching unit EMV examines the content  
22 of the multimedia message directed to the target terminal  
23 device (cf.  $\Phi$ ). If said message contains DRM-protected  
24 useful data objects and contained therein in turn are the  
25 reference and signaling for the functionality according to  
26 the invention for adapting DRM-protected contents to the  
27 characteristics of the target terminal device, the MMS  
28 switching unit EMV sends a request to the data provisioning  
29 component DBK of the content provider. The request contains  
30 either the DRM container object CO itself or an identifier  
31 for the DRM container object (e.g. a content URI) and in  
32 addition the description of the target terminal device  
33 characteristics. The data provisioning component DBK

1 analyzes the target terminal device characteristics,  
2 establishes whether the DRM-protected content NDO currently  
3 contained in the multimedia message is suitable for the  
4 target terminal device, whether it can provide a more  
5 suitable variant as an alternative, or whether a suitable  
6 variant of the DRM-protected content cannot be provided.  
7 According to the result of the analysis, the data  
8 provisioning component DBK sends a response message  
9 containing information to the MMS switching unit EMV in  
10 which either the suitability of the already present DRM  
11 container object is confirmed or the DRM-protected content  
12 is made available in a more suitable form, or it is signaled  
13 by means of an error message that neither is the present  
14 DRM-protected content suitable nor can it be made available  
15 in an alternative suitable form. If the DRM-protected  
16 content is to be made available in a more suitable form,  
17 this can be accomplished either by direct integration into  
18 the response from the data provisioning component DBK to the  
19 MMS switching unit EMV, or only a reference or a pointer is  
20 integrated into the response, via which reference/pointer  
21 the MMS switching unit EMV can start a separate transaction  
22 for retrieving the DRM-protected content in a suitable form  
23 from the data provisioning component DBK. This is  
24 represented in Fig. 2 as a separate, dashed pair of arrows  
25 with the designation "4a".

26

27 5. After the DRM-protected object or all DRM-protected  
28 objects NDO has/have been checked in an MM and where  
29 appropriate replaced or (due to lack of compatibility with  
30 the target terminal device) removed, the MM is delivered by  
31 the MMS switching unit in the conventional manner (cf. γ).  
32 First, a recipient notification I concerning the provision,  
33 on the MMS switching unit EMV, of a multimedia message which

1 is to be transmitted and which contains a useful data object  
2 is sent to the MMS user application ENA. The MMS user  
3 application ENA responds in the variant shown with a  
4 delivery request II to the MMS switching unit EMV, which in  
5 turn delivers the multimedia message by MMS delivery message  
6 III.

7  
8 6. The multimedia message together with the encrypted or  
9 DRM-protected useful data object NDO has arrived at the MMS  
10 user application and can be used. A DRM license, which is  
11 referred to as a rights object RO, is required in order to  
12 use DRM-protected contents or useful data objects. Said  
13 rights object RO is either already present on the target  
14 terminal device TG2 or is downloaded separately for the DRM-  
15 protected object(s) in the multimedia message by the target  
16 terminal device TG2 (cf. η). The content or the useful data  
17 object can subsequently be used or displayed on the target  
18 terminal device, with the DRM-specific rights and  
19 restrictions being taken into account.

20  
21 In the final analysis the method ensures that the contents  
22 or useful data objects contained in a multimedia message -  
23 even if they are subject to DRM protection and are possibly  
24 encrypted - are transmitted to the target terminal device  
25 only in a form that is suitable for this device. Thus, the  
26 use of the transmission capacity from the MMS switching unit  
27 EMV to the MMS user application ENA on the terminal device  
28 is optimized and a means is provided to prevent the user of  
29 the target terminal device TG2 from receiving DRM-protected  
30 objects which he or she cannot use with his or her terminal  
31 device.

1 As already described above, the entire functionality is  
2 built on an additional information element (reference) in  
3 the encrypted useful data object or in the container object  
4 CO for the DRM-protected content. Conventionally, a possible  
5 format for the container is described in the specification  
6 "OMA-Download-DRMCF-v1\_0 - DRM Content Format". According to  
7 this, a container object for a DRM-protected content is  
8 structured as shown in Fig. 3.

9  
10 The container object CO is basically divided into 2 areas.  
11 The first contains control information SI and meta data  
12 relating to the content of the container, while the second  
13 area contains the DRM-protected content NDO in encrypted  
14 form. The control information SI includes the version of the  
15 specification to which the container corresponds, length  
16 specifications relating to the field "ContentType" and  
17 "ContentURI", the field "ContentType", which designates the  
18 type and format of the DRM-protected content in the  
19 container, the field "ContentURI", which contains a unique  
20 identifier for the present container object, and the "RI-  
21 URI", a reference to the rights provider which is used by a  
22 terminal device in order to download new rights objects (DRM  
23 licenses). The new element according to the invention is  
24 referred to as the "Transcoding-URI" and contains a  
25 reference to a resource via which a transaction according to  
26 the above description relating to step  $\Phi$  can be performed.  
27 In this case the transaction runs as an automated process  
28 and is based on defined requests and responses/answers with  
29 defined status codes and error messages. Interventions by  
30 human operators are not necessary either on the MMS  
31 switching unit EMV side or on the side of the data  
32 provisioning component DBK of the content provider. Further  
33 information can follow in additional header fields. The 2nd

1 part of the container contains the useful data object/the  
2 content in encrypted form.

3  
4 The integration of the new signaling information or  
5 reference in the field "Transcoding-URI" is also possible  
6 alternatively for other container formats for DRM-protected  
7 contents. It is accomplished in an analogous manner for  
8 formats defined in the future. In the case of an individual  
9 useful data object in a container object an individual  
10 element of signaling information is sufficient; with a  
11 plurality of objects in a DRM container object, an  
12 individual element of signaling information can also be  
13 assigned to each useful data object in order to allow an  
14 individual check to be made per useful data object.

15

16